UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/609,011	06/30/2003	Jari Karjala	004770.00133	8337

22907 7590 04/02/2007	EXAMINER
BANNER & WITCOFF, LTD. 1100 13th STREET, N.W. - SUITE 1200 WASHINGTON, DC 20005-4051	NGUYEN, MINH DIEU T

ART UNIT	PAPER NUMBER
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

	Application No.	Applicant(s)
Office Action Summary	10/609,011	KARJALA ET AL.
	Examiner	**Art Unit**	
	Minh Dieu Nguyen	2137	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 January 2007*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47* is/are pending in the application.

  4a) Of the above claim(s) *48* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

  Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

  Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

  a)☐ All b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

  * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
  Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
  Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This office action is in response to the communication dated 1/10/07 with the election of group I (claims 1-47) and the cancellation of claim 48.

2.   Claims 1-47 are pending.

Claim Objections

3.   Claims 1-3, 5, 9, 14, 20, 24-27, 29, 33, 38, 40 and 44 are objected to because of the following informalities:

        a)   As to claims 1 and 25, the phrase "configuration information for the at least one program" should be "configuration information for the at least one **local application** program"; "configuring the at least one program" should be "configuring the at least one **local application** program".

        b)   As to claims 2 and 26, the phrase "the information received in step (d)" should be "the **configuration** information received in step (d)".

        c)   As to claims 3 and 27, the phrase "an update to the at least one application program" should be "an update to the at least one **local** application program".

        d)   As to claims 5 and 29, the phrase "without PKI data" should be "without **public key infrastructure (PKI)** data".

        e)   As to claims 9 and 33, the phrase "on behalf other application programs" should be "on behalf **of** other application programs".

f)   As to claims 14 and 38, the phrase "fetching new or updated content from

the remote device" should be. "fetching new or updated content **to** the remote device".

g)   As to claims 20 and 44, the phrase "a message is the last message"

should be "a message is **a** last message".

h)   As to claim 24, the phrase "the recipient to verify the signature and identify

and authenticate the sender" should be "**a** recipient to verify the signature and identify

and authenticate **a** sender".

i)   As to claim 29, the phrase 'the device of claim 1" should be "the device of

claim **25**".

j)   As to claim 40, the phrase 'the device of claim 7" should be "the device of

claim **31**".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

4.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly
claiming the subject matter which the applicant regards as his invention.

5.   Claims 1-48 are rejected under 35 U.S.C. 112, second paragraph, as being

indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention.

In claims 1 and 25, step (d) "receiving, in response to step (c) and if the at least

one local application program is not configured, configuration information for the at least

one program" is not clear, it fails to particularly point out and distinctly claim the subject

matter. The limitation could be interpreted as receiving configuration information anyway

and if the one local application program is not configured, then configure it based on the

received configuration information (step (e)) or receiving configuration information if the

one local application program is not configured, then configure it based on the received

configuration information (step (e)). In the specification, paragraph [0007] discloses if

the local application program is not configured, a second process is initiated to access a

database to receive the configuration information. The examiner, as best understood,

interprets this limitation as disclosed in the specification.

Claim Rejections - 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

7.   Claims 1-2 and 25-26 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Cheline et al. (2003/0041136).

        a)   As to claim 1, as best understood, Cheline discloses a method for

implementing secure communication (i.e. implementing a virtual private network (VPN)

between a client-side system and a server-side system, see Cheline: 0001), comprising:

(a) receiving instructions to initiate a process for creating a secure communication link

to a remote device via a publicly accessible network (i.e. based on commands and

information entered by remote corporate VPN system administrators, the VPN provider

dispatches instructions to configure and control the modem 106 and a VPN

concentrator 136, see Cheline: 0033; the modem 106 is coupled to one or more remote

client computers 102 (1)-(N), see Cheline: Fig. 1, elements 102(1)-(N), 106); (b)

determining, in response to the instructions received in step (a), whether at least one

local application program used to create the secure communication link is configured

(i.e. security settings are determined for the client-side system based at least partially

on the data, see Cheline: 0016, once the security settings are determined, it anticipates

that local application program (e.g. configuration data) are also determined, see

Cheline: 0006); (c) initiating, based on the instructions received in step (a), a second

process for accessing a database over the publicly accessible network (i.e. the VPN

provider couples to a value added network services (VANS) database, see Cheline: Fig.

1, elements 118, 128; the VANS database provides the features that allow management

of the entire VPN, the VANS database contains the security policies and certificates for

the modem 106 and the VPN concentrators 136, the VANS database contains server

location information, network information or the like. The network information preferably

includes DNS server addresses, authentication server addresses, WINS server IP

addresses, default corporate network subnets, encryption and authentication

algorithms, user's configuration information (locations, additional corporate subnets

allowed to connect to), or the like, see Cheline: 0038); (d) receiving, in response to step

(c) configuration information for at least one program (i.e. VPN configuration details,

including the security settings, are then transmitted to the client-side system, see

Cheline: 0016); (e) configuring the at least one program based upon the configuration

information received in step (d) (i.e. the client side system uses the configuration details

to configure itself to establish a secure VPN tunnel between the server side system and

itself, see Cheline: 0016) and (f) creating the secure communication link based on the

configuration (i.e. a virtual private network tunnel is subsequently established between

the client-side system and the server-side system, see Cheline: 0016).

Cheline is silent on the capability of having if the at least one local application

program is not configured. However Cheline discloses how corporations provide VPN

connectivity to their employees must go through a number of set-up steps comprising

the server operator must set up the individual's account on the server side and

configure the client-side by manually entering the configuration data, etc. (see Cheline:

0006). It anticipates that the local application program (e.g. configuration data) must be

set up for implementing a VPN connection, therefore it anticipates that if the local

application program is not configured, the configuration information is received.

It would have been obvious to one of ordinary skill in the art at the time of the

invention to employ the use of having if at least on local application program is not

configured, (receiving configuration information for the at least one local application

program), in the system of Cheline so as to properly and automatically configuring the

client and server for VPN communication (see Cheline: 0001).

b)   As to claim 2, Cheline discloses the method of claim 1 wherein the secure

communication link is a VPN connection (i.e. a VPN is a private data network that

makes use of tunnels to maintain privacy when communicating over a public

telecommunication infrastructure, such as the Internet. Data communicated on a VPN is

encrypted before being sent through the public network and decrypted at the receiving

end, see Cheline: 0004-0005) and the information received in step (d) comprises at

least one of a public/private key pair and a certificate (i.e. security settings are

determined for the client-side system and security settings preferably include public and

private keys and/or a digital certificate, see Cheline: 0016).

       c)   As to claim 25, this claim is directed to a hardware implementation of the

method of claim 1 and is rejected by a similar rationale applied against claim 1 above.

       d)   As to claim 26, this claim is directed to a hardware implementation of the

method of claim 2 and is rejected by a similar rationale applied against claim 2 above.

8.   Claims 3 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Cheline et al. (2003/0041136) in view of Tuomenoksa et al. (7,028,333).

       a)   As to claim 3, Cheline discloses the method of claim 1, however he is

silent on the capability of determining whether an update to the at least one application

program is available; receiving the update and implementing the update. Tuomenoksa

is relied on for the teaching of determining whether an update to the at least one

application program is available; receiving the update and implementing the update (i.e.

the network operations center provides information and code for configuring processors,

such as computers as gateways capable of participating in one or more virtual private

networks; administering the configuration of the virtual private networks, distributing

changes to the configuration of the virtual private networks; disseminating software

updates to the gateways, see Tuomenoksa: col. 22, lines 12-30). It would have been

obvious to one of ordinary skill in the art at the time of the invention to employ the use of

determining whether an update to the at least one application program is available;

receiving the update and implementing the update in the system of Cheline, as

Tuomenoksa teaches, so as to provide a cost, time and complexity effective virtual

private networks (see Tuomenoksa: col. 3, lines 53-58).

b)   As to claim 27, this claim is directed to a hardware implementation of the

method of claim 3 and is rejected by a similar rationale applied against claim 3 above.

9.   Claims 4-5 and 28-29 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Cheline et al. (2003/0041136) in view of Balaz et al. (7,100,046).

a)   As to claim 4, Cheline discloses the method of claim 1, wherein the secure

communication link is a VPN connection (i.e. a VPN is a private data network that

makes use of tunnels to maintain privacy when communicating over a public

telecommunication infrastructure, such as the Internet. Data communicated on a VPN is

encrypted before being sent through the public network and decrypted at the receiving

end, see Cheline: 0004-0005), step (b) comprises determining if a client certificate is

present (i.e. before information is transferred between parties, both sides need to

authenticate themselves by using digital certificates, see Cheline: 0027, it anticipates

the client certificate is present, and further the VANS database contains the security

policies and certificates for the modem 106 and the VPN concentrators, see Cheline:

0038, therefore the client certificate is determined to be present in the system).

However he is silent on the capability of requesting enrollment of a client certificate if a

client certificate is not present and receiving a client certificate. Balaz is relied on for the teaching of requesting enrollment of a client certificate if a client certificate is not present and receiving a client certificate (i.e. to participate in a VPN, router enrolls for a certificate, see Balaz: col. 2, lines 10-11 and the certificate authority determines whether to trust the source of the request and responds with the requested certificate, see Balaz: col. 2, lines 15-18). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of requesting enrollment of a client certificate if a client certificate is not present and receiving a client certificate in the system of Cheline, as Balaz teaches, so as to provide secure communications by obtaining and maintaining certificates for a VPN (see Balaz: col. 1, lines 11-16).

   b)   As to claim 5, Cheline discloses the method of claim 1, wherein step (d) comprises having a generic VPN policy without PKI data (i.e. the step of generating PKI data is disclosed by Cheline (see below) indicates initially the system does not have a VPN policy with PKI data) and further comprising: (g) generating PKI data (i.e. security settings are then automatically determined for the client-side, the security settings preferably include public and private keys and/or a digital certificate, see Cheline: 0016) and a corresponding certificate enrollment request (addressed by Balaz, see claim 4 above). Cheline is silent on the capability of sending the certificate enrollment request to the remote device for forwarding to an external certification authority (CA); and receiving a certificate. Balaz is relied on for the teaching of sending the certificate enrollment request to the remote device for forwarding to an external certification authority (CA); and receiving a certificate (i.e. router sends a GetCertificate request and the certificate

is then returned by certificate authority to registration authority, who returns the

certificate to router (see Balaz: col. 13, lines 15-61). It would have been obvious to one

of ordinary skill in the art at the time of the invention to employ the use of sending the

certificate enrollment request to the remote device for forwarding to an external

certification authority (CA); and receiving a certificate in the system of Cheline, as Balaz

teaches, so as to provide secure communications by obtaining and maintaining

certificates for a VPN (see Balaz: col. 1, lines 11-16).

     c)   As to claim 28, this claim is directed to a hardware implementation of the

method of claim 4 and is rejected by a similar rationale applied against claim 4 above.

     d)   As to claim 29, this claim is directed to a hardware implementation of the

method of claim 5 and is rejected by a similar rationale applied against claim 5 above.

10.   Claims 6 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Cheline et al. (2003/0041136) in view of Balaz et al. (7,100,046) and further in view of

Dickinson et al. (6,853,988).

     a)   As to claim 6, the combination of Cheline and Balaz discloses the method

of claim 4, however it is silent on the capability of wherein the received client certificate

is enrolled, in cooperation with an internal corporate certification authority, with an

external certification authority. Dickinson is relied on for the teaching of wherein the

received client certificate is enrolled, in cooperation with an internal corporate

certification authority, with an external certification authority (i.e. enrollment process

may issues multiple digital certificates from multiple certificate authorities, including one

or more proprietary certificate authorities internal or external to the trust engine, see

Dickinson: col. 20, lines 48-55). It would have been obvious to one of ordinary skill in

the art at the time of the invention to employ the use of wherein the received client

certificate is enrolled, in cooperation with an internal corporate certification authority,

with an external certification authority in the system of Cheline and Balaz, as Dickinson

teaches, so as to securely perform remote requests for cryptographic functions on a

server (see Dickinson: col. 3, lines 11-13).

      b)   As to claim 30, this claim is directed to a hardware implementation of the

method of claim 6 and is rejected by a similar rationale applied against claim 6 above.

11.   Claims 7-10, 12-14, 22, 31-34, 36-38 and 46 are rejected under 35 U.S.C. 103(a)

as being unpatentable over Cheline et al. (2003/0041136) in view of Whelan et al.

(2004/0203593).

      a)   As to claim 7, Cheline discloses the method of claim 1, however he is

silent on the capability of initiating an automatic content update (ACU) application.

Whelan is relied on for teaching of initiating an automatic content update (ACU)

application (i.e. the configuration management server can also distribute software and

stored data updates to the mobile units, see Whelan: 0047). It would have been obvious

to one of ordinary skill in the art at the time of the invention to employ the use of

initiating an automatic content update (ACU) application in the system of Cheline, as

Whelan discloses, so as to create, update and manage hardware and software profiles

for mobile units (see Whelan: 0011).

b)   As to claim 8, the combination of Cheline and Whelan discloses the

method of claim 7, wherein the ACU application contains information about application

programs in addition to the at least one local application program used to create the

secure communication link (i.e. capabilities under configuration management can

include: ...VPN software, ...software applications, see Whelan: 0025-0032), and further

comprising: determining whether an update is available for at least one of the additional

application programs; and receiving an update for the at least one additional application

program (i.e. when changes to configuration profiles, data or software become

available, the configuration management will notify the configuration management client

of the pending synchronization, see Whelan: 0065).

c)   As to claim 9, the combination of Cheline and Whelan discloses the

method of claim 7, wherein the ACU application communicates with the remote device

and other remote device on behalf other application programs (i.e. the one or more

servers may have the capabilities to update software modules and stored data, see

Whelan: 0040).

d)   As to claim 10, the combination of Cheline and Whelan discloses the

method of claim 7, wherein the ACU application contains information about application

programs in addition to the at least one local application program used to create the

secure communication link (i.e. capabilities under configuration management can

include: ...VPN software, ...software applications, see Whelan: 0025), and further

comprising: fetching from the remote device content or content metadata applicable to

at least one of the additional application programs (i.e. ...the one or more configuration

management servers propagates changes in data, software or configuration profiles to the mobile units, the configuration management client on the mobile unit will periodically poll the server to determine if synchronization is required, see Whelan: 0065) and storing by the at least one additional application program, the fetched content or content metadata (i.e. the changes are transmitted through the access point to the configuration management clients on the mobile unit, which updates the effected files, see Whelan: 0065).

       e)   As to claim 12, the combination of Cheline and Whelan discloses the method of claim 7, further comprising: storing, in a configuration record for at least one application, an Internet Access Point to be used when communicating with a remote device on behalf of the at least one application (i.e. the configuration policy changes dynamically with the access point, whenever a mobile unit connects to a new access point, the system invokes and verifies the proper configuration profile for that access point, see Whelan: 0025).

       f)   As to claim 13, the combination of Cheline and Whelan discloses the method of claim 7, wherein the ACU application communicates using a simple request-response protocol, and wherein a protocol transaction consists of a single request-response pair (i.e. request for updated information (i.e. synchronization), see Whelan: 0037, 0065).

       g)   As to claim 14, the combination of Cheline and Whelan discloses the method of claim 7, wherein the ACU application contains information about application programs in addition to the at least one local application program used to create the

secure communication link, and further comprising: fetching from the remote device content metadata applicable to at least one of the additional application program (i.e. the client periodically polls the configuration management server to determine if some of the profile information, software or stored data needs to be synchronized with the information stored on the configuration management server, see Whelan: 0078); comparing fetched metadata to locally stored metadata and fetching new or updated content from the remote device based upon the comparison (i.e. the configuration management client then synchronizes the configuration management profiles, software and data with the profiles, software and data on the configuration management server, see Whelan: 0080).

h)   As to claim 22, the combination of Cheline and Whelan discloses the method of claim 7, further comprising, upon receipt of a first response from the remote device, validating and storing a returned certificate to create a trust relationship with the remote device (i.e. the modem and the VPN concentrator validate each other's signature in the certificate, see Cheline: 0081-0082, and storing the certificate, see Cheline: 0064).

i)   As to claim 31, this claim is directed to a hardware implementation of the method of claim 7 and is rejected by a similar rationale applied against claim 7 above.

j)   As to claim 32, this claim is directed to a hardware implementation of the method of claim 8 and is rejected by a similar rationale applied against claim 8 above.

k)   As to claim 33, this claim is directed to a hardware implementation of the method of claim 9 and is rejected by a similar rationale applied against claim 9 above.

l)   As to claim 34, this claim is directed to a hardware implementation of the

method of claim 10 and is rejected by a similar rationale applied against claim 10 above.

m)   As to claim 36, this claim is directed to a hardware implementation of the

method of claim 12 and is rejected by a similar rationale applied against claim 12 above.

n)   As to claim 37, this claim is directed to a hardware implementation of the

method of claim 13 and is rejected by a similar rationale applied against claim 13 above.

o)   As to claim 38, this claim is directed to a hardware implementation of the

method of claim 14 and is rejected by a similar rationale applied against claim 14 above.

p)   As to claim 46, this claim is directed to a hardware implementation of the

method of claim 22 and is rejected by a similar rationale applied against claim 22 above.

12.   Claims 11 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Cheline et al. (2003/0041136) in view of Whelan et al. (2004/0203593) and further

in view of Berger et al. (7,114,126).

a)   As to claim 11, the combination of Cheline and Whelan discloses the

method of claim 7, however it is silent on the capability of having the ACU application

communicates using a SyncML protocol. Berger is relied on for the teaching of having

the ACU application communicates using a SyncML protocol (i.e. architecture 300

includes a file and data synchronization application 310, residing on application server

112, they communicate in SyncML - an XML-based open standard that specifies the

protocol for synchronizing heterogeneous devices – in order to exchange and resolve

file and data changes between master database and client's data store, see Berger: col.

9, lines 26-35). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the ACU application communicates using a SyncML protocol in the system of Cheline and Whelan, as Berger teaches, so as to provide a real time observation assessment in computer information gathering and processing.

b)   As to claim 35, this claim is directed to a hardware implementation of the method of claim 11 and is rejected by a similar rationale applied against claim 11 above.

13.   Claims 15-16 and 39-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cheline et al. (2003/0041136) in view of Whelan et al. (2004/0203593) and further in view of Terada et al. (7,113,983)

a)   As to claim 15, the combination of Cheline and Whelan discloses the method of claim 14, however he is silent on the capability of having the ACU application includes in fetch requests in steps (g) and (i) content identifications (IDs) required by the remote device. Terada is relied on for the teaching of having the ACU application includes in fetch requests in steps (g) and (i) content identifications (IDs) required by the remote device (i.e. the client station sends the content ID of the selected program file to the program serving site A, upon receipt of the content ID, site A searches through the content database for content files corresponding to the content ID, ...then sends thus-created information file to the client station, see Terada: col. 12, line 62 to col. 13, line 14). Terada is silent on having the content ID in step (i), content ID is information identifying one particular content, it is necessary in the request message (which is

disclosed by Terada), in the response message it could be implemented to confirm the requested item. It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the ACU application includes in fetch requests in steps (g) and (i) content identifications (IDs) required by the remote device in the system of Cheline and Whelan, as Terada teaches, so as to receive the specified content via a communication network (see Terada: col. 2, lines 45-52).

       b)   As to claim 16, the combination of Cheline and Whelan discloses the method of claim 7, wherein the ACU application contains information about applications programs in addition to the at least one local application program used to create the secure communication link (i.e. capabilities under configuration management can include: ...VPN software, ...software applications, see Whelan: 0025), however it is silent on the capability of fetching, from multiple databases in the remote device, metadata about multiple types of content. Terada is relied on for the teaching of fetching, from multiple databases in the remote device, metadata about multiple types of content (i.e. number of program files are prestored in each of sites A-N, and multiples types of content (e.g. music, picture) are sent from these multiple databases, see Terada: col. 8, lines 1-20). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of fetching, from multiple databases in the remote device, metadata about multiple types of content in the system of Cheline and Whelan, as Terada teaches, so as to download content files over a communication network.

c)   As to claim 39, this claim is directed to a hardware implementation of the

method of claim 15 and is rejected by a similar rationale applied against claim 15 above.

d)   As to claim 40, this claim is directed to a hardware implementation of the

method of claim 16 and is rejected by a similar rationale applied against claim 16 above.

14.   Claims 17 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Cheline et al. (2003/0041136) in view of Whelan et al. (2004/0203593) and further

in view of Shannon (6,233,618).

a)   As to claim 17, the combination of Cheline and Whelan discloses the

method of claim 7, wherein the ACU application contains information about application

programs in addition to the at least one local application program used to create the

secure communication link (i.e. capabilities under configuration management can

include: ...VPN software, ...software applications, see Whelan: 0025), and the ACU

application transmits requests, however it is silent on the capability of having the ACU

application transmits requests containing properties used by the remote device to filter

requests. Shannon is relied on for the teaching of having the ACU application transmits

requests containing properties used by the remote device to filter requests (i.e. when

user's request includes an Internet access address that appears in one of the

category/restricted database 208, then user will be denied access to that data, file,

applet, web page and so forth, see Shannon: col. 8, lines 6-12). It would have been

obvious to one of ordinary skill in the art at the time of the invention to employ the use of

having the ACU application transmits requests containing properties used by the remote

device to filter requests in the system of Cheline and Whelan, as Shannon teaches, so

as to provide access control based upon the requests (see Shannon: col. 4, lines 26-

30).

b)   As to claim 41, this claim is directed to a hardware implementation of the

method of claim 17 and is rejected by a similar rationale applied against claim 17 above.

15.   Claims 18, 21, 42 and 45 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Cheline et al. (2003/0041136) in view of Whelan et al.

(2004/0203593) and further in view of Peterka et al. (2003/0140257).

a)   As to claim 18, the combination of Cheline and Whelan discloses the

method of claim 7, however it is silent on the capability of having messages generated

by the ACU application and communicated to the remote device include a message

identifier, a target database identifier, and a security level. Peterka is relied on for the

teaching of having messages generated by the ACU application and communicated to

the remote device include a message identifier, a target database identifier, and a

security level (i.e. content provider generates a session rights object (SRO)

encapsulates the purchased options (i.e. content ID is included) selected by the

consumer, an optional set of content access rules (e.g. security level), the content

provider then redirects the viewer to the appropriate caching server (i.e. a target

database identifier), see Peterka: 0063-0065). It would have been obvious to one of

ordinary skill in the art at the time of the invention to employ the use of having

messages generated by the ACU application and communicated to the remote device

include a message identifier, a target database identifier, and a security level in the system of Cheline and Whelan, as Peterka teaches, so as to securely deliver content to legitimate customers (see Peterka: 0013).

b)   As to claim 21, the combination of Cheline, Whelan and Peterka discloses the method of claim 18, wherein the ACU application requests configuration information in a single message (see Whelan: 0093).

c)   As to claim 42, this claim is directed to a hardware implementation of the method of claim 18 and is rejected by a similar rationale applied against claim 18 above.

d)   As to claim 45, this claim is directed to a hardware implementation of the method of claim 21 and is rejected by a similar rationale applied against claim 21 above.

16.   Claims 19 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cheline et al. (2003/0041136) in view of Whelan et al. (2004/0203593) in view of Peterka et al. (2003/0140257) and further in view of Redlich et al. (7,103,915).

a)   As to claim 19, the combination of Cheline, Whelan and Peterka discloses the method of claim 18, however it is silent on the capability of having a first security level is required to receive configuration information for the at least one program and a second security level is required to receive another type of information. Redlick is relied on for the teaching of having a first security level is required to receive configuration information for the at least one program and a second security level is required to receive another type of information (i.e. the multiple levels and standards or security is introduced, wherein the level of security is determined by the extent of the security

sensitive items, selection process, the extent of dispersal to various distributed storage locations; the rules for controlled-release from storage; and the access rules governing the reconstitution of extracts into the secured document, see Redlich: col. 8, lines 21-26, users with low level security only are permitted to have access to low level extracted data and users with high level security are permitted to access the entire document, see Redlich: col. 7, lines 12-17). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having a first security level is required to receive configuration information for the at least one program and a second security level is required to receive another type of information in the system of Cheline, Whelan and Peterka, as Redlich teaches, so as to provide flexibility in controlling content delivering (see Redlich: col. 8, lines 43-48).

      b)   As to claim 43, this claim is directed to a hardware implementation of the method of claim 19 and is rejected by a similar rationale applied against claim 19 above.

17.   Claims 20 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cheline et al. (2003/0041136) in view of Whelan et al. (2004/0203593) in view of Peterka et al. (2003/0140257) and further in view of Traversat et al. (2002/0152299).

      a)   As to claim 20, the combination of Cheline, Whelan and Peterka discloses the method of claim 18, however it is silent on the capability of having at least one message generated by the ACU application includes an element indicating that a message is the last message relating to a specific task. Traversat is relied on for the teaching of having at least one message generated by the ACU application includes an

element indicating that a message is the last message relating to a specific task (i.e. a message may include an indication that it is the last message, see Traversat: 0184). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having at least one message generated by the ACU application includes an element indicating that a message is the last message relating to a specific task in the system of Cheline, Whelan and Peterka, as Traversat teaches, so as to provide reliable connections between peers in a peer-to-peer networking environment, see Traversat: 0007).

b)   As to claim 44, this claim is directed to a hardware implementation of the method of claim 20 and is rejected by a similar rationale applied against claim 20 above.

18.   Claims 23-24 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cheline et al. (2003/0041136) in view of Whelan et al. (2004/0203593) and further in view of Srinivasan (2003/0126085).

a)   As to claim 23, the combination of Cheline and Whelan discloses the method of claim 22, however it is silent on the capability of using the returned certificate to validate subsequent responses from the remote device. Srinivasan is relied on for the teaching of using the returned certificate to validate subsequent responses from the remote device (i.e. the information cached remains in the recipient's local keystore and is available for processing of subsequently received message, see Srinivasan: 0047). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of using the returned certificate to validate subsequent responses from

the remote device in the system of Cheline and Whelan, as Srinivasan teaches, so as to make message communication more efficient without repeating authentication of certificates, see Srinivasan: 0047).

b)   As to claim 24, the combination of Cheline, Whelan and Srinivasan discloses the method of claim 23, wherein the returned certificate is validated based on a hash calculated over the entire ACU message resulting in the first response from the remote device, except for a signature element of the ACU message (e.g. a cryptographic digest of the message (i.e. excluding signature element), see Srinivasan: 0003, 0040), the hash is signed with a private key held by the remote device (i.e. sender A encrypts (i.e. signs) a cryptographic digest of the message using its private key, see Srinivasan: 0003), and the corresponding certificate is included in the first response and is used by the recipient to verify the signature and identify and authenticate the sender (i.e. assuming that a recipient B of the message has the sender's public key, the recipient can apply the sender's public key to decrypt the message digest, then by comparing the decrypted digest to a computed digest of the received message, the recipient can authenticate the message to verify that the message originated with sender A and that the message was not altered after sender A sent it, see Srinivasan: 0003).

c)   As to claim 47, this claim is directed to a hardware implementation of the method of claim 23 and is rejected by a similar rationale applied against claim 23 above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

mdn
3/27/07